

FIG. 1

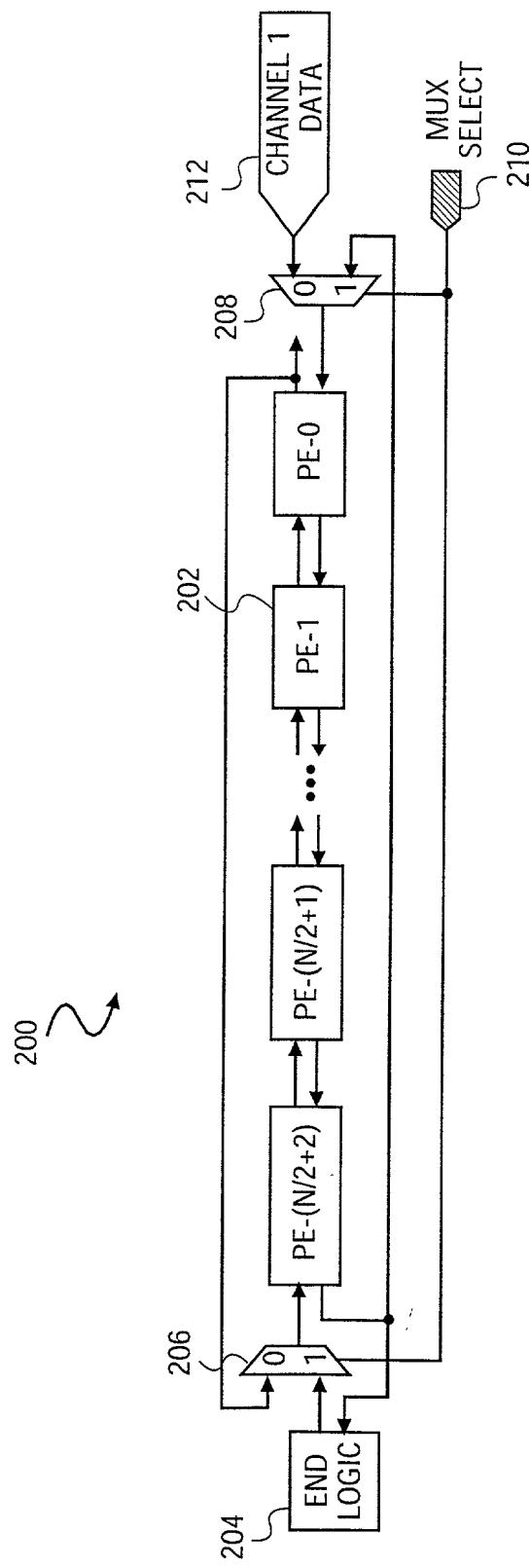


FIG. 2

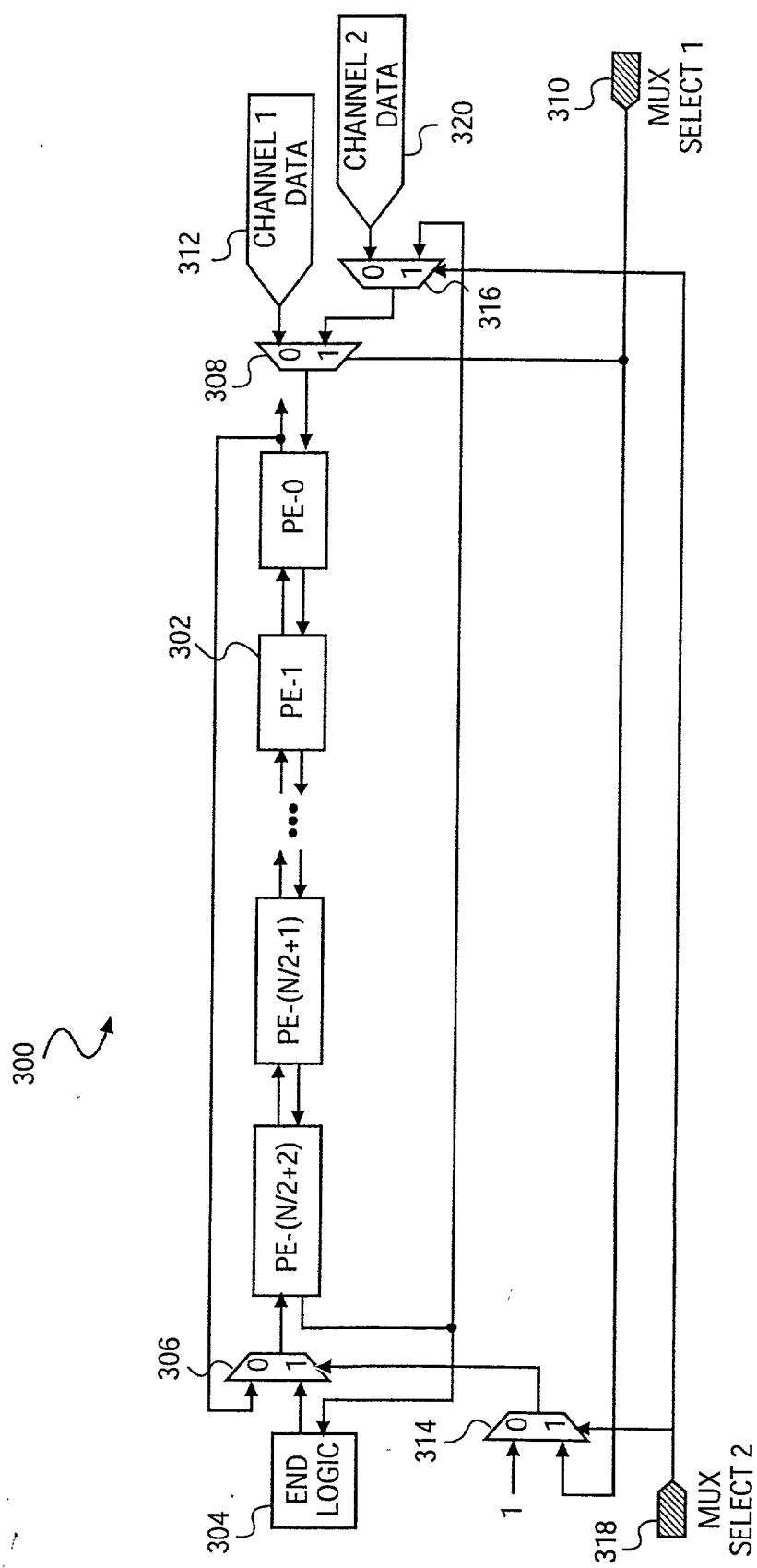


FIG. 3

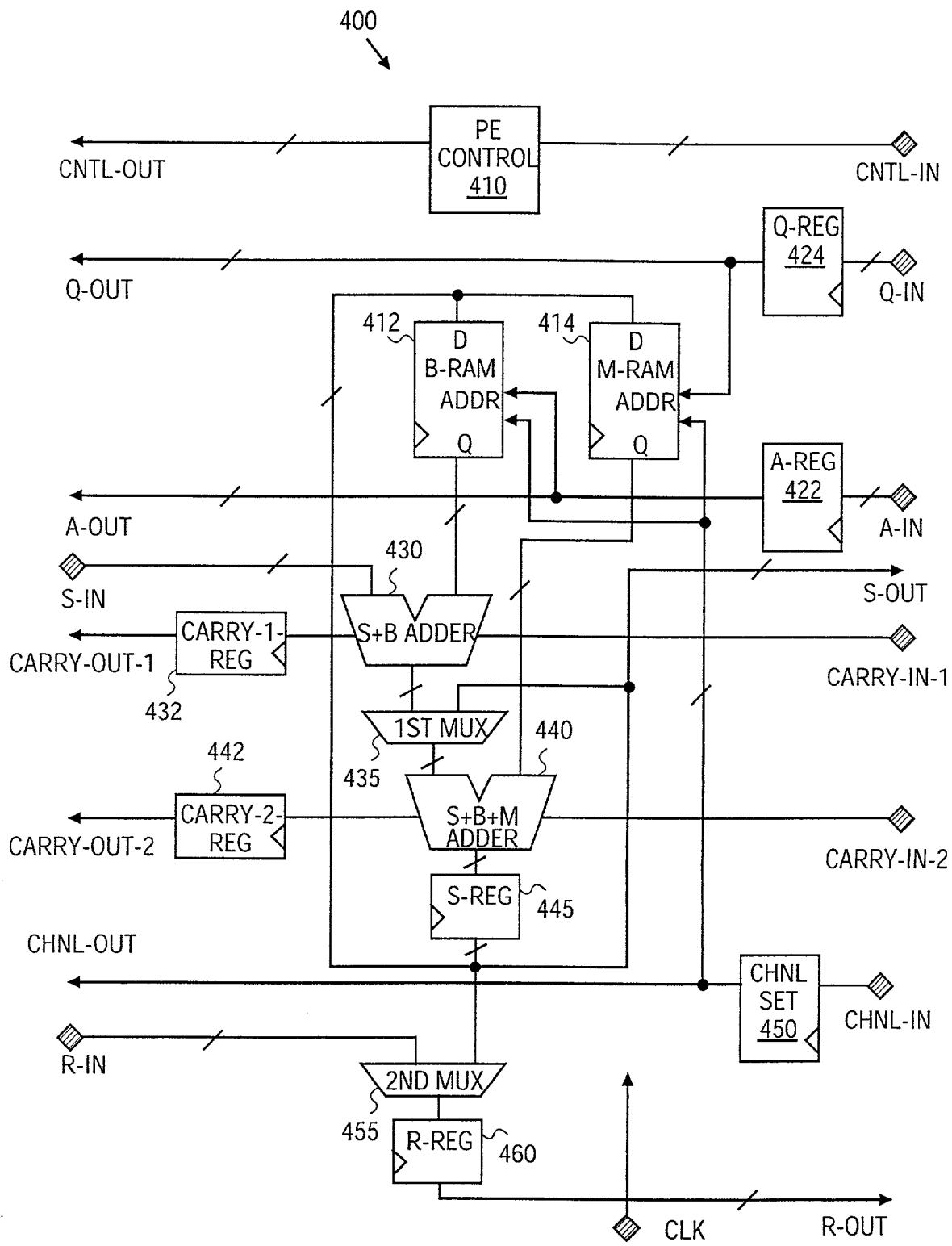


FIG. 4

TITLE: METHOD AND APPARATUS FOR PERFORMING MODULAR MULTIPLICATION
INVENTOR(S): MICHAEL D. RUEHLE
ATTY. DOCKET NO.: 042390.P11975

5/6

CYCLE	MUX SELECT	END LOGIC	PE-6	PE-5	PE-4	PE-3	PE-2	PE-1	PE-0	INPUT REGS
1	0									
2	1								0	
3	0							1	0	
4	1						2	0	0	
5	0					3	1	0	0	
6	1				4	2	1	0	0	
7	0			5	3	1	0	0	0	
8	1		6	4	2	1	0	0	0	
9	0		5	3	2	0	0	0	0	
10	1		6	4	3	0	0	0	0	
11	0		5	3	1	0	0	0	0	
12	1		6	4	10	0	0	0	0	
13	0		5	11	3	0	0	0	0	
14	1		6	12	4	0	0	0	0	
15	0		13	5	11	3	0	0	0	
16	1		6	12	4	10	0	0	0	
17	0		13	5	11	3	0	0	0	
18	1		6	12	4	10	0	0	0	
19	0		13	5	11	3	0	0	0	
20	1		6	12	4	10	0	0	0	

FIG. 5

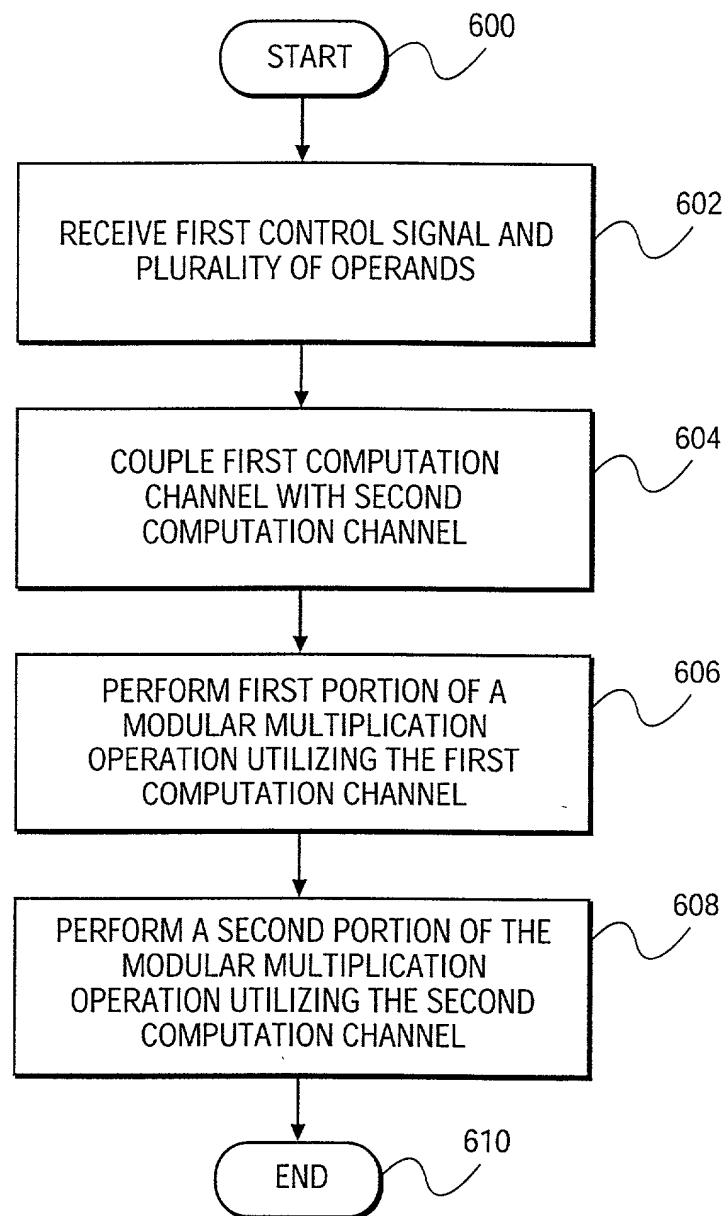


FIG. 6